Dark Web 101

Major Jeremy Cole, USAF

Today's internet has multiple webs. The surface web is what Google and other search engines index and pull based on links. Essentially, the surface web is the master index of publically available indexes providing returns to searches based on search terms and links. The surface web is small at only 4%. The second, called the deep web, consists of roughly 96% or the rest of the web. The deep web consists of protected sites that require users to input data to get access (email or online banks), unlinked content (unpublished blogs or organizational databases), proprietary data (study results, financial records, research & development), and personal data (medical records or legal documents). These are all deep web. Standard search engines don't have access to these sites and therefore cannot search them. The last web is the dark web, a part of the deep web. It requires specific software, logins, and knowledge to access. This is home to hidden sites that prefer to stay in the dark.

What do a hacker, a government investigative agency, EUROPOL, an anonymous source reporting to a journalist, a dissident in a country where free speech is repressed, drug dealers, pedophiles, hit men for hire, a whistle blower, a privacy zealot, and terrorists have in common? They all depend on online anonymity to ensure privacy, protect personal information, enable freedom of expression, or paradoxically, to censor it. Additionally, they also rely on online anonymity to conduct illicit activities. Whether to communicate, surf the web or host data, these individuals and organizations conduct their activities on the dark web to keep hidden from public view. What the dark web is, how it works and primarily who uses it is essential to understanding that it represents a mixed bag of hidden services consisting of many different personalities from across all swaths of society.

What is it?

Some call the dark web "the seedy underbelly of the Internet where you can buy drugs, weapons, child pornography, [and] murders-for-hire."[1] Others highlight how "it helps political dissidents who want to evade government censors."[2] In either case, the dark web is a collection of hard to find websites because it's "not indexed by search engines such as Google and not easily navigated to using a standard web browser."[3] A quick outline of its technical development and evolution give definition to this discussion. In a general sense, the dark web, aka darknet, hides internet activity of the individuals that use it to communicate, host data or access a specific website. Traditionally, internet access depends on an internet service provider (ISP) to connect its users to the internet. The ISPs assign Internet Protocol (IP) addresses to its users and data hosts. IP addresses provide organizational details about the ISP, its geographic location, closest city, websites visited, and other identifying information called metadata. The dark web enables its users and data hosts to anonymously surf the web, host a website or communicate using a global network that obfuscates its users' IP addresses. This anonymity concept relies on software the Naval Research Lab (NRL) developed in 2002. In 2004, NRL released the second generation of 'the onion router' or Tor as it's more commonly known. By May 2004, Tor had "32 nodes (24 in the US, 8 in Europe).[4]"Today's Tor network numbers over 6000 nodes[5] making it the largest internationally and the primary tool used to access the dark web.

While the anonymity Tor provided darknet users was beneficial, the dark web has since gained other uses – some legal, some not. For example, according to one of Tor's original developers, Michael Reed, Tor initially had legitimate aims "The *PURPOSE* [sic] was for DoD [US Depart-

ment of Defense] / Intelligence usage…not assisting dissidents…criminals [or] bit-torrent users…."[6] However, nine years after its second-generation launch, University of Luxembourg researchers using Tor evaluated almost 40,000 hidden Tor sites. In summary, they "found that the content of Tor hidden services is rather varied. The number of hidden services with illegal content or devoted to illegal activities and the number of other hidden services (devoted to human rights, freedom of speech, anonymity, security, etc.) is almost the same."[7] Interestingly, their analysis found an almost even numerical divide between legitimate (56%) versus illicit (44%) sites.[8] Given the broad reach of Tor nodes globally, it's fair to assert that not all is bad on the darknet. The US Government invested roughly $1.8 million[9] in Tor in 2013. Additionally, Tor is now "an open source project run by volunteers and supported by activists, nonprofit organizations, universities and governments."[10] These factors together suggest that Tor and the dark web in which it resides may not be as rife with crime and illegality as previously thought. Despite differing opinions, the dark web exists so individuals, intentions aside, can anonymously communicate, host data or surf the web. Naturally, the dark web and its tools have evolved to include a broad range of activity but remain focused on anonymity.

How does it work?

The dark web uses encryption and anonymizing software to protect its users and data hosts. Use of encryption among dark web users is not new. For example, the Islamic State of Iraq and the Levant (ISIL) reportedly began experimenting with encryption tools as early as November 2013.[11] Two years later, further reporting says ISIL now has "a 24-hour "help desk" to advise burgeoning jihadists on encrypting their communications in order to evade authorities." Open source reporting with specifics on ISIL encryption techniques is sparse, especially when related to attack planning. For example, it was initially believed that ISIL used encryption to plan the Paris attacks. However, later information clarified that the reported planning using PlayStation4's encryption was false. In the latest ISIL-motivated attack in San Bernadino, there's no current public information saying encryption was involved in the planning. However, according to Aaron F. Brantly of the US Army-affiliated Combating Terrorism Center there are at least "120 separate [communication] platforms, many of them encrypted…creating a space…to operate independent of direct surveillance." While these examples highlight may negative uses, encryption does have redeeming value in protecting everything done online today from paying your cable bill, managing your finances, perusing favorite websites, commenting on social media, sharing opinions important to you, to listening to your favorite music online. Because encryption is essential in protecting the authenticity of personal information and ensuring only those authorized gain access, anonymizing software will continue to rely on it.

How to access the dark web?
-Download an anonymizing software (like Tor)
-Follow installation instructions
-Launch browser (it should **connect** automatically)
-Go to a directory of hidden services to begin (like the Hidden wiki)

Primarily, the dark web combines encryption with anonymizing software (AS) to hide its users and data hosts. Tor is the most common AS on the dark web though there are other options like virtual private networks (VPNs), peer-to-peer (P2P), or the Invisible Internet Project (I2P). There are many techniques to hide identity using an AS. For example, Tor "encrypt[s] web traffic [the 'where you want to go online' process] in layers and bounce[s] it through randomly-chosen computers around the world [6000 nodes available referenced previously], each of which removes a single layer of encryption before passing the data on to its next hop in the network." This process called 'hopping' hides the Tor user and data host's IP addresses routing them through three random points making identification of origin very difficult. When running a website via Tor, both user IP and web server hop three times versus VPNs that only hop once.

Another common technique called spoofing makes it look like your IP is somewhere else. This is quite useful for gaining access to specific online resources (TV shows, shopping, newsfeeds, etc.) only available in a given physical location based on IP address. For example, using a VPN one can access Netflix, a US-based company, while living in Italy and using an Italian ISP. VPNs allow customers to choose IPs in multiple nations throughout the world enabling access to online resources anonymously. VPNs are quite popular because they're "free and are often faster than browsing via the Tor network, as well as being much easier to use." Anonymizing software and encryption offer users and data hosts the ability to hide their identity securely. Because encryption ensures authorized access only to unique data, dark web users rely on it. When paired with software like Tor or a VPN that hide one's identity, the chances of remaining anonymous are greatly increased thus protecting the identity of users or data hosts.

Who uses it?

Be advised!

-Access to illegal services and or content is just a click away.
-You cannot "unsee" content.
-Portrayals of violent death, actual deaths & suicides are common place.
-Psychological impacts can result.

This is a tricky question to answer since most dark web users prefer to remain anonymous. However, considering the number of internet users, available websites, what and how darknet users browse, dark web use, which is infinitesimally small, is a mixed bag. For example, currently, there are over 3.2 billion Internet users globally compared to Tor's claim of 2 million daily users. Assuming Tor numbers are accurate; this means .0625% of internet users get around the web using Tor. Concluding that all 2 million use Tor to access the dark web to sell drugs or look at child abuse images is foolhardy. Numbers from Tor say "only 1.5% of overall traffic...[has] to do with hidden sites." With close to 1 billion sites online, Tor estimates range from 7000 to 30,000. In other words, Tor's dark web contribution is approximately .03% of the overall web. These numbers suggest a very small dark web community of users, data hosts and available data. According to the Tor project this community includes "normal people" interested in protecting themselves from "unscrupulous marketers and identity thieves...Reporters without borders, Voice of America/Radio Free Europe/Radio Free Asia...Citizen journalists in China...Law enforcement officers...whistleblowers...business executives...bloggers...[and] military...for field agents, hidden services and Intelligence gathering" among others." Presumably, these folks use the darknet via Tor to protect their online activities. There are others on the darknet the Tor project didn't mention. For example, two years ago an individual set up an assassination market targeting politicians in exchange for bitcoin. Another example are hackers marketing their services. There appears to be a catch though because "in order to establish a business relationship, hackers must be polite to their clients, complete their surreptitious tasks in a timely fashion, and in some cases, even offer money-back guarantees." Conversely, there are well-minded individuals like the hacker called 'Intangir', "who became a champion for the dark web last March [2014] when he hacked into the Hidden Wiki, and deleted all of the links to child pornography." Another example is Doctor X, a trained physician that helps people decrease drug dependencies. He set up a site to help drug marketplace users. He said "People ask me about the real risks and adverse effects, [of] drug combinations [illegal and prescriptive] and the use of drugs in persons suffering from different conditions, such as diabetes or neurological problems." These altruistic actions offer hope that human decency can exist in anonymity.

Given the small number of darknet users and online offerings, reviewing popular content to understand darknet users based on available data offers mixed results. For example, reporting from the Internet Watch Foundation (IWF) found "31,266 URLs [uniform resource locator or link to an online resource] that contained child porn images[1]." Of those, the IWF said "In 2014,

we identified 51 previously unseen hidden services distributing child sexual abuse content, an increase of 55% over 2013[2]." The hidden illicit content, a mere 0.002%, is not as troubling as the increase in use of hidden services to push child sex abuse content. This suggests an increase in child sex abuse rings extant via the darknet. A second example illustrates darknet drug vendor habits. In November 2014, legal and judicial authorities from 17 nations[3] cracked down on darknet drug marketplaces in an operation dubbed 'Operation Onymous.' The operation included 17 arrests, the seizure of 414 .onion [Tor hosted] domains, "more than $1 million in bitcoin [digital currency used online without any legitimate banking institutional involvement], $250,000 in cash,[4]" other assets and multiple online drug marketplace seizures. The operation was successful, but as "the most popular drug site [the Silk Road] on the dark web[5]," went down, others took its place. Sites like Agora flourished offering "more than 16,000 mostly-illegal products[6]." Fast forward six months and figures from 24 April 2015, confirm that smaller darknet drug marketplace sites "experience[d] significant growth over the last month[7]." It appears the drug market actually expanded thanks to the void created by the Silk Road takedown. This activity implies that drug marketplaces continued and possibly even increased their darknet presence after Operation Onymous. Interestingly, Agora, a major dark web drug marketplace, recently closed its operations over concerns "that vulnerabilities in Tor's hidden services could lead to its servers being located[8]." Based on these examples and recalling the conclusions of the University of Luxembourg study previously mentioned, we can conclude that the darknet community is small, continues to push illegal activity despite continued law enforcement crack downs and makes every effort to protect itself from discovery based on the latest technological trends.

Common Darknet Sites

Drugs: Brainmagic, Agora Phishing, Mom4Europe, Exit Seven, CocaineMarket, DreamMarket

Hardware: Hackintosh, TorGameDepot, Underground Electronics

Counterfeits: USD Counterfeits, Cheap Euros, 20 Dollar USD Notes

Weapons: European Arms, GlobalGuns, Black Market

Passports: United States Citizenship , UK Passports

Other: Rent-A-Hacker, Hitman Network, Bitcoin Financial, CloneCards, SocialHack, Silkroad Phishing

Darknet tactics vary making it hard to identify darknet users or data hosts. For example, Dr. Gareth Owen, University of Portsmouth professor, conducting a six-month study of hidden TOR sites found that 75% of dark web users visited child abuse sites. Owen questioned the numbers however, because "Most of the hidden services we only saw once. They do not tend to exist for a very long time[9]." Owen's findings confirm that a basic tactic of illicit websites is to relocate on a regular basis. It then follows that ongoing access to these sites requires diligent, deliberate contact with the data host to have the latest location of the real site. Another common tactic is to use fake, or scam, sites. Not knowing which sites are real and which are dummy sites, complicates policing efforts. For example, one report about Operation Onymous claims almost half the sites seized and closed down were either fake or scam-related[10]." Thus, this tactic affords darknet users protection in an environment where one "could be a click away from sites selling drugs and guns, and - frankly - even worse things[11]." Another tactic, using VPNs in an environment where censorship reigns, enables darknet communication. One Chinese blogger who established a darknet blog said "This is a free Chinese Internet world, here you can speak whatever is on your mind[12]." Another responded excitedly to the post saying "I feel nervous even now, because of my timid personally. I never thought my first contact with the dark web would be on a Chinese website. I hope the webmaster continues their good work[13]." These tactics reflect user's concerns about protecting their identity to avoid getting caught doing something illicit or considered illegal. To summarize, numbers show that overall the dark web community–users and sites offered–is barely a drop in the proverbial "internet" bucket. The evaluation of website visits offers little to help define darknet users giving only mixed results because of tactics that mask activity.

Increasing awareness of the dark web and how it works is not as difficult as defining who the darknet community is. Originally, the darknet served legitimate US government purposes providing protection for individuals conducting investigations, fieldwork and intelligence collection. However, individuals seeking to capitalize on criminal activity enabled the darknet to flourish primarily using Tor. Interestingly, Tor designers expected this to happen mentioning that there "would be other unavoidable uses for the technology...and if those uses were going to give us more cover traffic to better hide what we wanted to use the network for, all the better[14]." The darknet depends on encryption and anonymity to protect its users and data hosts. Data encryption is an ancient, gold-standard of protection assuring only authorized individuals gain access to verifiable, unchanged data. The use of anonymizing software coupled with encryption provides complex, powerful protection to the dark web community. When compared to the aggregate number of internet users, darknet users are almost nonexistent. Additionally, the number of available darknet web sites versus standard websites is paltry – about the size of an electron on the head of a pin in the hand of a basketball player standing at mid court in the Alamodome in San Antonio, Texas. Given the nature of the dark web, defining its users is hard. Available information suggests a few user types – computer savvy individuals whose tactics help them avoid legal tangles, computer savvy individuals motivated by altruism and plain old users simply interested in protecting their personal information. In today's interconnected global world, the darknet community will most likely continue to grow in popularity reflecting a society of legal and moral conundrums apparently deciphered by no one specifically.

Notas

1. https://www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_Report_14_web.pdf, page 9, accessed 10 December 2015.
2. Ibid, page 17.
3. https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network, accessed 2 December 2015.
4. http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/, accessed 10 December 2015.
5. http://www.wired.com/2014/11/feds-seize-silk-road-2/, accessed 15 December 2015.
6. Ibid.
7. http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet, accessed 11 December 2015.
8. http://www.scmagazine.com/dark-website-agora-closes-over-tor-vulnerability-suspicions/article/435278/, accessed 15 December 2015.
9. http://www.bbc.com/news/technology-30637010, accessed 12 December 2015
10. http://techcrunch.com/2014/11/18/nearly-half-of-the-operation-onymous-takedowns-were-scam-or-clone-sites/, accessed 12 December 2015.
11. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/, accessed 16 December 2015
12. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community, accessed 2 December 2015
13. Ibid.
14. https://cryptome.org/0003/tor-spy.htm, accessed 10 December 2015.
15. http://www.nbcnews.com/storyline/paris-terror-attacks/are-isis-geeks-using-phone-apps-encryption-spread-terror-n464131, accessed 8 December 2015.
16. http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, accessed 25 November 2015.
17. Ibid.
18. Ibid.
19. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community, accessed 2 December 2015
20. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/, accessed 2 December 2015.
21. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community, accessed 2 December 2015
22. http://www.internetlivestats.com/watch/internet-users/, accessed 9 December 2015.
23. http://www.wired.com/2015/06/dark-web-know-myth/, accessed 9 December 2015.
24. Ibid.
25. http://www.internetlivestats.com/total-number-of-websites/, accessed 12 December 2015.
26. Ibid.
27. Ibid.
28. https://www.torproject.org/about/torusers.html.en, accessed 11 December 2015.

29. http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/, accessed 11 December 2015.
30. http://www.ibtimes.co.uk/new-breed-lone-wolf-hackers-are-roaming-deep-web-their-prey-getting-bigger-1483347, accessed 11 December 2015.
31. http://www.ibtimes.co.uk/how-cyber-vigilantes-catch-paedophiles-terrorists-lurking-deep-web-1479291, accessed 11 December 2015.
32. Ibid..
33. https://www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_Report_14_web.pdf, page 9, accessed 10 December 2015.
34. Ibid, page 17.
35. https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network, accessed 2 December 2015.
36. http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/, accessed 10 December 2015.
37. http://www.wired.com/2014/11/feds-seize-silk-road-2/, accessed 15 December 2015.
38. Ibid.
39. http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet, accessed 11 December 2015.
40. http://www.scmagazine.com/dark-website-agora-closes-over-tor-vulnerability-suspicions/article/435278/, accessed 15 December 2015.
41. http://www.bbc.com/news/technology-30637010, accessed 12 December 2015.
42. http://techcrunch.com/2014/11/18/nearly-half-of-the-operation-onymous-takedowns-were-scam-or-clone-sites/, accessed 12 December 2015.
43. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/, accessed 16 December 2015.
44. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community, accessed 2 December 2015.
45. Ibid.
46. https://cryptome.org/0003/tor-spy.htm, accessed 10 December 2015.

"The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government."

Major Jeremy Cole (BA, Weber State University in Spanish, MA, University of Kansas) is currently a Course Director for the eSchool of Graduate PME at Maxwell AFB, AL. As a career intelligence officer, he has worked at multiple levels including Combatant Command.

DARPA

When you do a simple Web search on a topic, the results that pop up aren't the whole story. The Internet contains a vast trove of information – sometimes called the "Deep Web" – that isn't indexed by search engines: information that would be useful for tracking criminals, terrorist activities, sex trafficking and the spread of diseases. Scientists could also use it to search for images and data from spacecraft. The Defense Advanced Research Projects Agency (DARPA) has been developing tools as part of its Memex program that access and catalog this mysterious online world. Researchers at NASA's Jet Propulsion Laboratory in Pasadena, California, have joined the Memex effort to harness the benefits of deep Web searching for science. Memex could, for example, help catalog the vast amounts of data NASA spacecraft deliver on a daily basis.

Elizabeth LandauJet
Propulsion Laboratory, Pasadena, California.